Everbridge SASB Index

Everbridge is dedicated to conducting business in a responsible manner that considers the impact on its operations, customers, partners, and global communities. The disclosures provided below serve to illustrate Everbridge's commitment to responsible business practices and reflect our alignment with the SASB Software and IT Services sector framework. We prioritize providing disclosures on the metrics that are most relevant to our business. In this index, we refer to existing disclosures or respond directly to the metrics. However, we do not currently report on all metrics, and in some cases, we only have partial information available. We are committed to evaluating new developments and adapting our disclosures accordingly.

Code	Description	Response
Environmental Footprint of Hardware Infrastructure		
TC-SI-130a.1	(1) Total energy consumed, (2) percentage grid electricity, (3) percentage renewable	Everbridge, as a cloud-based software provider, operates with a minimal carbon footprint. While we have not yet quantified the environmental footprint of our operations as a whole, we rely on hyperscale public cloud providers who have sustainability goals we directly benefit from, including: • 100% renewable energy by 2025 • Net-zero emissions by 2030 • Water positive by 2030 • Zero-waste by 2030 • 24/7 clean energy by 2030 • Net carbon-zero by 2040 • Power operations with 100% renewable energy by 2040 We monitor our cloud usage to drive efficiency improvements.
TC-SI-130a.2	(1) Total water withdrawn, (2) total water consumed, percentage of each in regions with High or Extremely High Baseline Water Stress	Our sustainability assessment determined that while we recognize the importance of responsible water management, water consumption does not emerge as a priority area based on our specific operational context. We will continue to monitor material environmental impacts as necessary moving forward.

TC-SI-130a.3	Discussion of the integration of environmental considerations into strategic planning for data center needs	See our publication, Unlocking Climate Change Resilience Through Critical Event Management and Public Warning, for information on how environmental considerations are incorporated into our strategic planning for data center needs and operational resilience.
Data Privacy & Freedom of Expression		
TC-SI-220a.1	Description of policies and practices relating to behavioral advertising and user privacy	As is true of most websites, we gather certain information automatically and store it in log files. This information includes internet protocol (IP) addresses, browser type, internet service provider (ISP), referring/exit pages, operating system, date/time stamp, and clickstream data. We may link this data with other information we collect from users to improve our offered services, marketing, analytics, and site functionality. However, we anonymize the data we link so that users cannot be identified. Refer to our Privacy Notice for more information.
TC-SI-220a.2	Number of users whose information is used for secondary purposes	We work to maintain compliance with the CCPA and GDPR in publishing privacy policies, marketing materials and other statements, including such as compliance with certain certifications or self-regulatory principles, regarding data privacy and security. Refer to our Privacy & Security webpage for more information.
TC-SI-220a.3	Total amount of monetary losses as a result of legal proceedings associated with user privacy	Refer to Item 3 "Legal Proceedings" in our 2022 Annual Report on Form 10-K for material litigation and regulatory matters.

TC-SI-220a.4	(1) Number of law enforcement requests for user information, (2) number of users whose information was requested, (3) percentage resulting in disclosure	Our company has established a standard protocol for handling requests from law enforcement agencies. We understand that privacy is a fundamental concern for our customers, and we are committed to striking a balance between safeguarding customer privacy and complying with law enforcement demands. To achieve this, our policy follows these key principles: 1. Strict Adherence to Legal Requirements: We conduct a legal review of law enforcement requests and will only respond to requests that are accompanied by valid legal documentation, such as a court-issued warrant, subpoena, or other lawful orders. 2. Narrow Disclosure: We will only disclose information that is explicitly required by the legal request. 3. Customer Notification: Whenever possible and within the boundaries of the law, we will notify affected customers when their data is requested by law enforcement, except when legally prohibited from doing so.
TC-SI-220a.5	List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring	We disclose the following processing locations for our core services: https://www.everbridge.com/about/legal/everbridge-sub-processors/
Data Security		
TC-SI-230a.1	Number of data breaches, (2) percentage involving personally identifiable information (PII), (3) number of users affected	Privacy & Security Policy Everbridge adheres to SEC requirements regarding the disclosure of material cybersecurity incidents.

TC-SI-230a.2	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	Everbridge conducts regular risk assessments to identify potential vulnerabilities and security gaps within its systems. These assessments involve evaluating potential threats, estimating their impact, and determining the likelihood of their occurrence. By conducting such assessments, Everbridge can proactively address vulnerabilities and minimize risks. Everbridge uses industry standard approaches identified in SOC-2, FedRAMP, and ISO 27001. For more information, refer to Privacy & Security Policy
Recruiting & Managing a Global, Diverse & Skilled Workforce		
TC-SI-330a.1	Percentage of employees that are (1) foreign nationals and (2) located offshore	(1) 1.05% of US-based employees are foreign nationals, (2) 48.64% of Everbridge employees are located offshore Everbridge mitigates potential risks (legal compliance with immigration laws and visa requirements, visa issues, and security concerns) of recruiting foreign nationals and/or offshore employees by conducting background checks on all potential employees and contractors, working with immigration attorneys to help navigate laws and regulations surrounding visas and work authorization requirements and monitoring visa expiration dates, and implementing security policies and protocols.
TC-SI-330a.2	Employee engagement as a percentage	Our annual survey was distributed in August 2023. We achieved a 71% participation rate in the annual survey. The survey results were shared with employees in a global All Hands call and via a series of department meetings & workshops. We have identified 2 global company-wide actions to address feedback and each department has a plan to address feedback at the department-level.

TC-SI-330a.3	Percentage of gender and racial/ethnic group representation for (1) management, (2) technical staff, and (3) all other employees	Please refer to our social section for detailed racial and ethnic data. We do not collect race/ethnicity data of employees outside of the US. The percentage listed is for US employees only. Technical staff includes all US employees under Architecture, Development, Corp IT, Security, Product Management, Quality & Release, and SaaS Ops.
Intellectual Property Protection & Competitive Behavior		
TC-SI-520a.1	Total amount of monetary losses as a result of legal proceedings associated with anti-competitive behavior regulations	Refer to Item 3 "Legal Proceedings" in our 2022 Annual Report on Form 10-K for material litigation and regulatory matters.
Managing Systemic Risks from Technology Disruptions		
TC-SI-550a.1	Number of (1) performance issues and (2) service disruptions; (3) total customer downtime	Please see the section titled "Risks Related to Cybersecurity and Reliability" in our 2022 Annal Report on Form 10-K for material risks we have identified surrounding performance, service disruptions and customer downtime.
TC-SI-550a.2	Description of business continuity risks related to disruptions of operations	Please see the section titled "Risks Related to Cybersecurity and Reliability" in our 2022 Annal Report on Form 10-K for risks related to disruptions of operations.